IN THE CLAIMS

1. (Previously Presented) A transmission system for providing conditional access to transmitted data; the system including a transmitter and a plurality of receivers coupled via a network;

the transmitter including means for transmitting:

to all receivers the same data encrypted under control of a same authorization key; and

to all receivers a same key block with a plurality of entries, wherein each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, and

each of the receivers being associated with a corresponding set of a plurality of device keys, wherein at least two of the receivers are associated with sets that comprise at least one corresponding device key,

each of the receivers including:

means for receiving the key block and the encrypted data;

a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key; and

a second decryptor for decrypting the encrypted data under control of the authorization key.

2. (Original) A transmission system as claimed in claim 1, wherein the set of device keys associated with each respective one of the receivers is unique for the receiver.

3. (Original) A transmission system as claimed in claim 1, wherein the transmitter is operative to disable decryption of the data in a receiver by changing the authorization key and transmitting a key block wherein entries associated with device keys which are associated with a receiver to be revoked contain values other than the representation of the authorization key encrypted with the associated device key.

4. (Previously Presented) A transmission system as claimed in claim 3, wherein the transmitter is operative to re-enable decryption of the data in a disabled receiver by changing the authorization key and transmitting a key block wherein at least one of the entries associated with device keys which are associated with a receiver to be re-enabled contains the representation of the authorization key encrypted with the associated device key.

5. (Original) A transmission system as claimed in claim 1, wherein the transmitter is operative to renew a set of device keys of a specific receiver by transmitting to the receiver a new set of device keys encrypted under control of a fixed device key that is unique for the receiver, and wherein the receiver is operative to receive a set of encrypted device keys, and the receiver includes a third decryptor for decrypting the set of encrypted device keys under control of a fixed device key that is unique for the receiver.

6. (Canceled)

7. (Previously Presented) A transmitter for use in a transmission system as claimed in claim 1, wherein the transmitter is coupled via the network to the plurality of receivers; the transmitter including the means for transmitting:

to all receivers the same key block with the plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, enabling the receivers to retrieving the authorization key by decrypting at least one entry of the key block that is associated with one of the set of device keys associated with the receiver; and

to all receivers same data encrypted under control of the same authorization key, enabling the receivers to retrieve the data by decrypting the data under control of the authorization key.

8. (Previously Presented) A receiver for use in a transmission system as claimed in claim 1, wherein the receiver is associated with the corresponding set of a plurality of device keys; the receiver including:

means for receiving encrypted data which is the same for all receivers in the system and which is encrypted under control of the authorization key which is the same for all receivers in the system;

means for receiving the key block which is the same for all receivers in the system; the key block including a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key,

the first decryptor for retrieving the authorization key by decrypting at least one entry of the key block that is associated with one of the set of device keys associated with the receiver;

the second decryptor for decrypting the data under control of the authorization key.

9. (Previously Presented) A transmission system for providing conditional access to transmitted data including:

a transmitter and a plurality of receivers coupled via a network;

the transmitter configured to transmit a same data stream encrypted under control of a same authorization key to all receivers and to all receivers a same key block with a plurality of entries, wherein each entry is associated with a different device key, at least one of the entries containing a representation of the authorization key encrypted with the associated device key, and

each of the receivers being associated with a corresponding set of a plurality of device keys and being configured to receive the key block and the encrypted data, with a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key and a second decryptor for decrypting the data under control of the authorization key.

10. (Previously Presented) A transmission system as defined in claim 9, wherein the set of device keys associated with each respective one of the receivers is unique for the receiver.

11. (Previously Presented) A transmission system as defined claim 9, wherein the transmitter is operative to disable decryption of the data in a receiver by changing the authorization key and transmitting a key block wherein entries associated with device keys which are associated with a receiver to be revoked contain values other than the representation of the authorization key encrypted with the associated device key.

12. (Previously Presented) A transmission system as defined in claim 11, wherein the transmitter is operative to re-enable decryption of the data in a disabled receiver by changing the authorization key and transmitting a key block wherein at least one of the entries associated with device keys which are associated with a receiver to be re-enabled contains the representation of the authorization key encrypted with the associated device key.

13. (Previously Presented) A transmission system as defined claim 9, wherein the transmitter is operative to renew a set of device keys of a specific receiver by transmitting to the receiver a new set of device keys encrypted under control of a fixed device key that is unique for the receiver, and wherein the receiver is operative to receive a set of encrypted device keys, and the receiver includes a third decryptor for decrypting the set of encrypted device keys under control of a fixed device key that is unique for the receiver.

14. (Canceled)

15. (Previously Presented) A transmitter for use in a transmission system as defined claim 9, wherein the transmitter is coupled via the network to the plurality of receivers; the transmitter including the means for transmitting:

to all receivers the same key block with a plurality of entries, wherein each entry is associated with a respective different device key and wherein each of the receivers is associated with a corresponding set of a plurality of device keys and wherein at least one of the device keys of the set corresponds to a device key of another receiver in the system, at least some of the entries containing a representation of the authorization key encrypted with the associated device

key, enabling the receivers to retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key, and

to all receivers same data encrypted under control of the same authorization key, enabling the receivers to retrieve the data by decrypting the data under control of the authorization key.

16. (Previously Presented) A receiver for use in a transmission system as defined claim 9, wherein the receiver is associated with the set of a plurality of device keys and wherein at least one of the device keys of the set corresponds to a device key of another receiver in the system, the receiver including:

means for receiving encrypted data which is the same for all receivers in the system and which is encrypted under control of the authorization key which is the same for all receivers in the system;

means for receiving the key block which is the same for all receivers in the system; the key block including a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key,

the first decryptor for retrieving the authorization key taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key;

the second decryptor for decrypting the data under control of the authorization key.

17. (Previously Presented) A transmission system as defined claim 9, wherein the same key block corresponds to a subset of different device keys contained within the transmitter.

18. (Previously Presented) A transmission system as defined claim 9, wherein the receiver uses the first decryptor and the key block to retrieve the authorization key.

19. (Previously Presented) A transmission system as defined claim 1, wherein the same key block corresponds to a subset of different device keys contained within the transmitter.

20. (Previously Presented) A transmission system as defined claim 1, wherein the receiver uses the first decryptor and the key block to retrieve the authorization key.

21. (Previously Presented) A method for providing conditional access to transmitted data over a network including a transmitter and a plurality of receivers, each of said receivers being associated with a corresponding set of a plurality of device keys, said method comprising:

transmitting the same data to all receivers, wherein said same data is encrypted under control of a same authorization key;

transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key;

receiving at each receiver the key block and the encrypted data, wherein each receiver is associated with a set of a plurality of device keys and wherein at least one of the device keys of the set corresponds with a device key of a set associated with another receiver in the system;

retrieving the authorization key at one or more of said plurality of receivers by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key; and

decrypting the data at said one or more of said plurality of receivers under control of the authorization key.

22. (Previously Presented) A method as claimed in claim 21, wherein the set of device keys associated with each respective one of the receivers is unique for the receiver.

23. (Previously Presented) The system of claim 1, wherein at least some device keys are shared between at least two of the receivers.

24. (Previously Presented) The system of claim 9, wherein at least some device keys are shared between at least two of the receivers.

25. (Previously Presented) A transmission system for providing conditional access to transmitted data; the system including a transmitter and a plurality of receivers coupled via a network;

the transmitter to transmit to all receivers the same data encrypted under control of a same authorization key; and

the transmitter to transmit to all receivers a same key block with a plurality of entries, wherein each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, and

each of the receivers being associated with a corresponding set of a plurality of device keys, wherein at least two of the receivers are associated with sets that comprise at least one corresponding device key, each of the receivers to receive the key block and the encrypted data and including:

a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key; and

a second decryptor for decrypting the encrypted data under control of the authorization key.